REMARKS

In the non-final Office Action, the Examiner objects to the oath/declaration and rejects claims 1-32 under 35 U.S.C. § 103(a) as unpatentable over BENNETT et al. (Quantum Cryptography: Public Key Distribution and Coin Tossing, International Conference on Computer Systems & Signal Processing, Bangalore India, 10-12 Dec. 1984) in view of LEE (U.S. Patent No. 5,535,195) and BASS et al. (U.S. Patent No. 4,649,233). Applicants respectfully traverse the objection and rejection. [1]

The declaration has been objected to as being defective because the signature of the first named inventor is found in the box intended for the second named inventor and because the declaration does not identify the mailing address of each inventor. In response, Applicants submit a new declaration herewith. As such, withdrawal of the objection to the declaration is respectfully requested.

Claims 1-32 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over BENNETT et al. in view of LEE and BASS et al. Applicants respectfully traverse this rejection.

Independent claim 1 recites a method of transporting a random block of bits in a quantum cryptographic key distribution (QKD) network. The method includes sharing blocks of bits between nodes in a QKD network using quantum cryptographic mechanisms; determining a key transport path between a source node and a destination node in the QKD network, wherein the key transport path comprises one or more intermediate nodes; at each intermediate node of the one or more intermediate nodes, logically combining a block of secret bits shared with a previous hop along the path with a block of secret bits shared with a next hop along the path to produce first combined blocks of bits; at the destination node, logically combining a block of secret bits shared with a previous hop along the path with a random block of bits to produce a second combined block

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine reference, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

of bits; receiving the first combined blocks of bits and the second combined block of bits at the source node; and logically combining, at the source node, the first combined blocks of bits and the second combined block of bits to determine the random block of bits. BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, BENNETT et al., LEE, and BASS et al. do not disclose or suggest logically combining a block of secret bits shared with a previous hop along a path with a block of secret bits shared with a next hop along the path to produce first combined blocks of bits at each intermediate node of one or more intermediate nodes; at the destination node, logically combining a block of secret bits shared with a previous hop along the path with a random block of bits to produce a second combined block of bits; receiving the first combined blocks of bits and the second combined block of bits at the source node; and logically combining, at the source node, the first combined blocks of bits and the second combined block of bits to determine the random block of bits. The Examiner admits that BENNETT et al. and LEE do not disclose these features and relies on column 6, lines 55-67 of BASS et al. as allegedly disclosing these features (Office Action, pp. 3-4). Applicants respectfully disagree with the Examiner's interpretation of BASS et al.

At column 6, lines 55-67, BASS et al. discloses:

> where + is addition modulo 2^{64} and where R1 * R2* R3* R4 represents a set of secret random numbers contributed by counterpart nodes. The fact that each node contributes its own random number in generating session keys ensures that session key generation scenarios cannot be "faked" by impostor nodes. This arises where the impostor nodes merely replay recordings of a previous key generation scenario.
>
> The R_n values are exchanged over the network just prior to the generation of the session key. In this regard, each node obtains a secret random number from each other node. Illustratively, suppose that there were only two nodes involved, x and y, and *KNC0 is stored at x and *KNC1 is stored at y.

This section of BASS et al. discloses that each of a plurality of nodes contributes its own random number in generating session keys, which ensures that session key generation scenarios cannot be "faked" by impostor nodes. This section of BASS et al. further discloses that the random numbers are exchanged over the network just prior to the generation of the session key, so each node obtains a secret random number from each other node. This section of BASS et al. merely discloses contributing random numbers when establishing session keys, not logically combining a block of secret bits shared with a previous hop along a path with a block of secret bits shared with a next hop along the path to produce first combined blocks of bits at each intermediate node of one or more intermediate nodes; at the destination node, logically combining a block of secret bits shared with a previous hop along the path with a random block of bits to produce a second combined block of bits; receiving the first combined blocks of bits and the second combined block of bits at the source node; and logically combining, at the source node, the first combined blocks of bits and the second combined block of bits to determine the random block of bits, as recited in claim 1.

For at least the foregoing reason, Applicants submit that claim 1 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Claims 2-6 depend from claim 1. Therefore, these claims are patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1.

Independent claim 7 recites a method of end-to-end transport of a secret key in a quantum cryptographic key distribution (QKD) network. The method includes determining multiple paths for end-to-end transport, employing QKD techniques, of the secret key across a QKD network; and transporting the secret key across each of the determined multiple paths. BENNETT et al., LEE, and BASS et al. do not disclose or suggest this combination of features.

For example, BENNETT et al., LEE, and BASS et al. do not disclose or suggest determining multiple paths for end-to-end transport, employing QKD techniques, of the secret key across a QKD network; and transporting the secret key across each of the determined multiple paths. The

Examiner admits that BENNETT et al. and LEE do not disclose this combination of features and relies on column 6, lines 45-50 of BASS et al. as allegedly disclosing these features (Office Action, pg. 7). Applicants respectfully disagree with the Examiner's interpretation of BASS et al.

At column 6, lines 45-50, BASS et al. discloses:

> Although the following example references two-node interconnection, the method of session key generation contemplates any number of nodes participating. Thus, irrespective of the number of nodes involved, all nodes should generate the same session key. The session key is defined by…

This section of BASS et al. discloses that, irrespective of the number of nodes involved, all nodes should generate the same session key. This section of BASS et al. does not mention a secret key, let alone determining multiple paths for end-to-end transport, employing QKD techniques, of the secret key across a QKD network; and transporting the secret key across each of the determined multiple paths, as recited in claim 7.

For at least the foregoing reason, Applicants submit that claim 7 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Claims 8-13 depend from claim 7. Therefore, these claims are patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 7.

Independent claim 14 recites a method of transporting a key between a first node at one end of a path through a quantum cryptographic key distribution (QKD) network to a second node at an opposite end of the path, the QKD network comprising a plurality of nodes. The method includes transmitting secret bits between the plurality of nodes of the QKD network using quantum cryptographic mechanisms; reserving, from the first node, portions of the transmitted secret bits at each intermediate node along the path between the first and the second node; and transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits. BENNETT et al, LEE, and BASS et al. do not disclose or suggest this combination of features.

For example, BENNETT et al, LEE, and BASS et al. do not disclose or suggest reserving, from a first node, portions of a transmitted secret bits at each intermediate node along the path between the first and the second node; and transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits. The Examiner admits that BENNETT et al. and LEE do not disclose these features and relies on column 6, lines 45-55 and column 7, lines 43-55 of BASS et al. as allegedly disclosing these features (Office Action, pg. 9). Applicants respectfully disagree with the Examiner's interpretation of BASS et al.

Column 6, lines 45-55 have been reproduced above. This section of BASS et al. discloses that, irrespective of the number of nodes involved, all nodes should generate the same session key. This section of BASS et al. does not mention secret bits, let alone reserving, from a first node, portions of a transmitted secret bits at each intermediate node along the path between the first and the second node; and transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits, as recited in claim 14.

At column 7, lines 43-55, BASS et al. discloses:

> For each node, the "last term" of both the R_n and PWF_n summations represents the random number value and user ID/password values of the local node. Also, for $n \geq 2$, a unique cross-domain pair is shared for each pair of nodes. Consequently, a compromise of one node does not operate to compromise the entire system.
>
> In the ensuing description, there is first set out a set of temporal and spatial definitions used in the example of the method of this invention. In this regard, the principal actions of the method are distributed over a timeline. These actions are symmetric such that each node mirrors the activity at the other node.

This section of BASS et al. discloses that a unique cross-domain pair is shared for each pair of nodes, so a compromise of one node does not operate to compromise the entire system. This section of BASS et al. further discloses that the actions of the nodes are symmetric such that each node mirrors the activity at the other nodes. This section of BASS et al. does not mention secret

bits, let alone reserving, from a first node, portions of a transmitted secret bits at each intermediate node along the path between the first and the second node; and transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits, as recited in claim 14.

For at least the foregoing reason, Applicants submit that claim 14 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Claims 15-22 depend from claim 14. Therefore, these claims are patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 14.

Independent claim 23 recites a computer-readable medium containing instructions for controlling at least one processor to perform a method of transporting a key across a quantum cryptographic key distribution (QDK) network. The method includes reserving portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network; and using the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent between nodes at either end of the path. BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, BENNETT et al., LEE, and BASS et al. do not disclose or suggest reserving portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network; and using the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent between nodes at either end of the path. The Examiner does not address these features when rejecting claim 23 (Office Action, pg. 11), thus a *prima facie* case of obviousness has not been established with respect to claim 23.

For at least the foregoing reason, Applicants submit that claim 23 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Claim 24 recites a node at a first end of a path in a quantum cryptographic key distribution (QKD) network that includes processing logic configured to: reserve portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network, and one or more interfaces configured to: receive the reserved portions of key symbols, the processing logic further configured to: use the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent to another node at a second end of the path. BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, BENNETT et al., LEE, and BASS et al. do not disclose or suggest processing logic configured to: reserve portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network, and one or more interfaces configured to: receive the reserved portions of key symbols, the processing logic further configured to: use the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent to another node at a second end of the path. The Examiner relies on column 6, lines 45-65 and column 7, lines 43-55 of BASS et al. as allegedly disclosing these features (Office Action, pp. 9 and 11). Applicants respectfully disagree with the Examiner's interpretation of BASS et al.

Column 6, lines 45-65 of BASS et al. have been reproduced above. This section of BASS et al. discloses that each node contributes its own random number in generating session keys. This section of BASS et al. does not disclose or suggest processing logic configured to: reserve portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network, and one or more interfaces configured to: receive the reserved portions of key symbols, the processing logic further configured to: use the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent to another node at a second end of the path, as recited in claim 24.

Column 7, lines 43-55 of BASS et al. have been reproduced above. This section of BASS et al. discloses that a unique cross-domain pair is shared for each pair of nodes, so a compromise of one node does not operate to compromise the entire system. This section of BASS et al. further discloses that the actions of the nodes are symmetric such that each node mirrors the activity at the other nodes. This section of BASS et al. does not disclose or suggest processing logic configured to: reserve portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network, and one or more interfaces configured to: receive the reserved portions of key symbols, the processing logic further configured to: use the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent to another node at a second end of the path, as recited in claim 24.

The disclosures of BENNETT et al. and LEE do not remedy the deficiencies in the disclosure of BASS et al. set forth above.

For at least the foregoing reasons, Applicants submit that claim 24 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Independent claim 25 recites a method of employing blocks of secret bits in communicating between a source node and a destination node in the network. The method includes transmitting the blocks of secret bits between each node along a path between the source node and the destination node using quantum cryptographic mechanisms, wherein a different block of secret bits of the blocks of secret bits is transmitted between each different link that connects each node along the path; initiating a reservation process, at the source node, the reservation process reserving at least a portion of the blocks of secret bits at each node along a path between the source node and the destination node; and employing the reserved blocks of secret bits in subsequent public communication between the source node and the destination node. BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, do not disclose or suggest this combination of features.

For example, BENNETT et al., LEE, and BASS et al. do not disclose or suggest initiating a reservation process, at a source node, the reservation process reserving at least a portion of a blocks of secret bits at each node along a path between the source node and a destination node; and employing the reserved blocks of secret bits in subsequent public communication between the source node and the destination node. The Examiner relies on column 6, lines 45-65 and column 7, lines 43-55 of BASS et al. as allegedly disclosing these features (Office Action, pg. 12). Applicants respectfully disagree with the Examiner's interpretation of BASS et al.

Column 6, lines 45-65 of BASS et al. has been reproduced above. This section of BASS et al. discloses that each node contributes its own random number in generating session keys. This section of BASS et al. does not disclose or suggest initiating a reservation process, at a source node, the reservation process reserving at least a portion of a blocks of secret bits at each node along a path between the source node and a destination node; and employing the reserved blocks of secret bits in subsequent public communication between the source node and the destination node, as recited in claim 25.

Column 7, lines 43-55 of BASS et al. has been reproduced above. This section of BASS et al. discloses that a unique cross-domain pair is shared for each pair of nodes, so a compromise of one node does not operate to compromise the entire system. This section of BASS et al. further discloses that the actions of the nodes are symmetric such that each node mirrors the activity at the other nodes. This section of BASS et al. does not disclose or suggest initiating a reservation process, at a source node, the reservation process reserving at least a portion of a blocks of secret bits at each node along a path between the source node and a destination node; and employing the reserved blocks of secret bits in subsequent public communication between the source node and the destination node, as recited in claim 25.

The disclosures of BENNETT et al. and LEE do not remedy the deficiencies in the disclosure of BASS et al. set forth above.

For at least the foregoing reasons, Applicants submit that claim 25 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination.

Claim 26 recites features similar to, yet possibly of different scope than, features recited above with respect to claim 25. Therefore, claim 26 is patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, for at least reasons similar to the reasons given above with respect to claim 25.

Claims 27-29 and 32 recite features similar to, yet possibly of different scope than, features recited above with respect to claim 1. Therefore, claims 27-29 and 32 are patentable over BENNETT et al., LEE, and BASS et al., whether taken alone or in any reasonable combination, for at least reasons similar to the reasons given above with respect to claim 1.

In view of the foregoing remarks, Applicant respectfully request reconsideration and allowance of pending claims 1-24.

If the Examiner believes that the application is not now in condition for allowance, Applicants respectfully request that the Examiner contact the undersigned to discuss any outstanding issues.

Applicant believes no fee is due with this response other than as indicated in the enclosed Amendment Transmittal. However, if a fee is due, please charge our Deposit Account No. 18-1945, under Order No. BBNT-P01-258 from which the undersigned is authorized to draw.

Dated: January 7, 2008

Respectfully submitted,

/Michael J. Chasan/
Michael J. Chasan
Registration No.: 54,026
ROPES & GRAY LLP
One International Place
Boston, Massachusetts 02110
(617) 951-7000
(617) 951-7050 (Fax)
Attorneys/Agents For Applicant